A Gentle Introduction to Quantum Information Science

Chi-Kwong Li
Department of Mathematics
The College of William and Mary
What is QIS?

Quantum properties
- Superposition
- Measurement effect
- Entanglement
- Decoherence
- Schrödinger cat

Quantum computing
- A brief history
- The computing model
- Computing by physical systems
- Mathematical formulation

Quantum Complexity
- Quantum algorithms

Quantum communication
- Quantum error correction
- Quantum cryptology
- Quantum teleportation

Conclusion

Thank you
What is QIS?

The study of information using quantum properties (effects).
What is QIS?

The study of information using quantum properties (effects).

Quantum Computing. Storage and processing of information.

Input → Computing Unit → Output
What is QIS?

The study of information using quantum properties (effects).

Quantum Computing. Storage and processing of information.

What is QIS?

The study of **information** using **quantum properties** (effects).

**Quantum Computing.** Storage and processing of information.

```
Input  →  Computing Unit  →  Output
```

**Quantum Communication.** Transmission of information.

**Quantum Complexity.** Efficiency in computing/communication.

```
Polynomial time  vs.  NP hard  vs.  BQP
```
What is QIS?

The study of information using quantum properties (effects).

Quantum Computing. Storage and processing of information.

\[
\text{Input} \rightarrow \text{Computing Unit} \rightarrow \text{Output}
\]


Quantum Complexity. Efficiency in computing/communication.

\[
\text{Polynomial time} \quad \text{vs.} \quad \text{NP hard} \quad \text{vs.} \quad \text{BQP}
\]

Let Dr. Quantum (Fred-Alan Wolf) explain some quantum properties useful for QIS.
Quantum properties

- **Superposition.**
  Useful in quantum computing/complexity; one can apply an operation simultaneously to many different physical states.
Quantum properties

- **Superposition.**
  Useful in quantum computing/complexity; one can apply an operation simultaneously to many different physical states.

- **Measurement effect, no cloning theorem.**
  Useful for the security of quantum communication (QKD); no eavesdropping and faking information.
Quantum properties

- **Superposition.**
  Useful in quantum computing/complexity; one can apply an operation simultaneously to many different physical states.

- **Measurement effect, no cloning theorem.**
  Useful for the security of quantum communication (QKD); no eavesdropping and faking information.

- **Quantum entanglement.**
  Useful for quantum computing, quantum communication such as quantum error correction, teleportation, superdense coding, etc.
Quantum properties

- **Superposition.**
  Useful in quantum computing/complexity; one can apply an operation simultaneously to many different physical states.

- **Measurement effect, no cloning theorem.**
  Useful for the security of quantum communication (QKD); no eavesdropping and faking information.

- **Quantum entanglement.**
  Useful for quantum computing, quantum communication such as quantum error correction, teleportation, superdense coding, etc.

- **Decoherence.**
  Quantum mechanical systems always try to interact with the environment causing additional probabilistic behaviors, and presenting challenges to quantum computing.
Superposition / Schrödinger cat

• In 1935, the Austrian physicist Erwin Schrödinger suggested a thought experiment showing that there was a problem with the Copenhagen interpretation of quantum mechanics (applied to everyday objects).
Superposition / Schrödinger cat

• In 1935, the Austrian physicist Erwin Schrödinger suggested a thought experiment showing that there was a problem with the Copenhagen interpretation of quantum mechanics (applied to everyday objects).

• The thought experiment presents a cat that might be simultaneously alive and dead with nonzero probability.
• In the course of developing his cat experiment, Schrödinger coined the term Verschränkung – literally, entanglement (mixing many cats!).
Entanglement

- In the course of developing his cat experiment, Schrödinger coined the term Verschränkung – literally, entanglement (mixing many cats!).

- If one has to handle/examine 10 cats each could be alive or dead, there are $2^{10} = 1024$ cases to study in classical information theory.
• In the course of developing his cat experiment, Schrödinger coined the term Verschränkung – literally, entanglement (mixing many cats!).

• If one has to handle/examine 10 cats each could be alive or dead, there are $2^{10} = 1024$ cases to study in classical information theory.

• In quantum information theory one can do it in one step!
Quantum computing

Motivations / a brief history

Quantum Information Science (QIS)
Chi-Kwong Li

What is QIS?
QC, QC, QC

Quantum properties
Superposition, Measurement effect, Entanglement, Decoherence, Schrödinger cat

Quantum computing
A brief history
The computing model
Computing by physical systems
Mathematical formulation

Quantum Complexity
Quantum algorithms

Quantum communication
Quantum error correction
Quantum cryptology
Quantum teleportation

Conclusion

Thank you
Quantum computing

Motivations / a brief history

- 1980’s R. Feynman suggested the use of quantum systems to do computing, and simulate more complex quantum systems.
Quantum computing

Motivations / a brief history

- 1980’s R. Feynman suggested the use of quantum systems to do computing, and simulate more complex quantum systems.
- 1990’s Quantum algorithms by Duestsch, Jozsa, Shor, etc. were proposed.
Quantum computing

Motivations / a brief history

- 1980’s R. Feynman suggested the use of quantum systems to do computing, and simulate more complex quantum systems.

- 1990’s Quantum algorithms by Duestsch, Jozsa, Shor, etc. were proposed. Shor’s quantum algorithm will have significant impact on the current (RSA) cryptology systems.
Quantum computing

Motivations / a brief history

- 1980’s R. Feynman suggested the use of quantum systems to do computing, and simulate more complex quantum systems.
- 1990’s Quantum algorithms by Duestsch, Jozsa, Shor, etc. were proposed. Shor’s quantum algorithm will have significant impact on the current (RSA) cryptology systems.
- 2000’s (Small scale) Quantum computers were/are built to test quantum algorithms.
Quantum computing

Motivations / a brief history

• 1980’s R. Feynman suggested the use of quantum systems to do computing, and simulate more complex quantum systems.
• 1990’s Quantum algorithms by Duestsch, Jozsa, Shor, etc. were proposed. Shor’s quantum algorithm will have significant impact on the current (RSA) cryptology systems.
• 2000’s (Small scale) Quantum computers were/are built to test quantum algorithms.
• A lot of advance in theory and physical implementation.
Quantum computing

Motivations / a brief history

• 1980’s R. Feynman suggested the use of quantum systems to do computing, and simulate more complex quantum systems.

• 1990’s Quantum algorithms by Duestsch, Jozsa, Shor, etc. were proposed. Shor’s quantum algorithm will have significant impact on the current (RSA) cryptology systems.

• 2000’s (Small scale) Quantum computers were/are built to test quantum algorithms.

• A lot of advance in theory and physical implementation.

• Still a long way to go, and many research needed to be done!
Quantum computing

Motivations / a brief history

- 1980’s R. Feynman suggested the use of quantum systems to do computing, and simulate more complex quantum systems.

- 1990’s Quantum algorithms by Duestsch, Jozsa, Shor, etc. were proposed. Shor’s quantum algorithm will have significant impact on the current (RSA) cryptology systems.

- 2000’s (Small scale) Quantum computers were/are built to test quantum algorithms.

- A lot of advance in theory and physical implementation.

- Still a long way to go, and many research needed to be done!

- Additional motivation. Transistors in digital computers are getting so small that quantum effects take place.
The computing model

The general model

Input  \rightarrow  \text{Computing Unit}  \rightarrow  \text{Output}
The computing model

The general model

Input → Computing Unit → Output

Classical computing.

Modern Computing
Quantum computing model

Quantum Computing Unit

Optical lattices, NMR
Quantum computing model

- Input - suitable quantum states as Quantum bits (Qubits).

Quantum Computing Unit
Optical lattices, NMR
Quantum computing model

- Input - suitable quantum states as Quantum bits (Qubits).
- A computing unit which can provide a suitable environment for the quantum algorithm to run (quantum system of qubits to evolve).
Quantum computing model

- **Input** - suitable quantum states as *Quantum bits (Qubits)*.
- **A computing unit** which can provide a suitable environment for the quantum algorithm to run (*quantum system of qubits to evolve*).
- **Output** - measure the resulting quantum states (*in a suitable way*) to get the useful information.
Computing by physical systems

Basic procedures

• Step 1. Set up the apparatus.
Computing by physical systems

Basic procedures

- Step 1. Set up the apparatus.

- Step 2. Let the system run.
Computing by physical systems

Basic procedures

- Step 1. Set up the apparatus.
- Step 2. Let the system run.
- Step 3. Do a suitable measurement to find the useful quantity.
Examples
Examples

- Use magnetic needle to find the north-south direction.
Examples

- Use magnetic needle to find the north-south direction.
- Set the length $L$ of the arm of the pendulum so that $2\sqrt{L/g} = 1$. Then the period $T$ of a full swing is $\pi$. 

\[ F = mg \]
Examples

- Use magnetic needle to find the north-south direction.

- Set the length $L$ of the arm of the pendulum so that $2\sqrt{L/g} = 1$. Then the period $T$ of a full swing is $\pi$.

- Put $1$ in the bank in 1960. Pay 2% annual interest rate deposited daily. In 2010 (50 years later), you get $e = 2.718281828459...$ (the Euler constant).
What is QIS?
QC QC QC

Quantum properties
Superposition, Measurement effect, Entanglement, Decoherence Schrödinger cat

Quantum computing
A brief history The computing model Computing by physical systems Mathematical formulation

Quantum Complexity
Quantum algorithms

Quantum communication
Quantum error correction Quantum cryptology Quantum teleportation

Conclusion

Thank you

Mathematical formulation

**Proposed by von Neumann**

- Consider a quantum system with two physical states, say, **up spin** and **down spin** of a particle represented by

Mathematics proposed by von Neumann.

- Consider a quantum system with two physical states, say, **up spin** and **down spin** of a particle represented by

Mathematics proposed by von Neumann.

- Consider a quantum system with two physical states, say, **up spin** and **down spin** of a particle represented by

Mathematics proposed by von Neumann.

- Consider a quantum system with two physical states, say, **up spin** and **down spin** of a particle represented by

Mathematics proposed by von Neumann.

- Consider a quantum system with two physical states, say, **up spin** and **down spin** of a particle represented by

Mathematics proposed by von Neumann.

- Consider a quantum system with two physical states, say, **up spin** and **down spin** of a particle represented by

Mathematics proposed by von Neumann.
### Mathematical formulation

#### Proposed by von Neumann

- Consider a quantum system with two physical states, say, **up spin** and **down spin** of a particle represented by

  \[
  |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.
  \]
Mathematical formulation

Proposed by von Neumann

- Consider a quantum system with two physical states, say, up spin and down spin of a particle represented by

\[ |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \]

- Before measurement, the vector state may be in superposition state represented by a complex vector

\[ v = |\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2, \quad |\alpha|^2 + |\beta|^2 = 1. \]
Mathematical formulation

Proposed by von Neumann

• Consider a quantum system with two physical states, say, up spin and down spin of a particle represented by

\[ |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \]

• Before measurement, the vector state may be in superposition state represented by a complex vector

\[ \psi = |\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2, \quad |\alpha|^2 + |\beta|^2 = 1. \]

• Thus the famous Schrödinger cat has probability \( |\alpha|^2 \) being alive and \( |\beta|^2 \) being dead!

Proposed by von Neumann

\[ |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \]

Before measurement, the vector state may be in superposition state represented by a complex vector

\[ \psi = |\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2, \quad |\alpha|^2 + |\beta|^2 = 1. \]

Thus the famous Schrödinger cat has probability \( |\alpha|^2 \) being alive and \( |\beta|^2 \) being dead!
Matrix and Bloch sphere

- It is convenient to represent the quantum state $|\psi\rangle$ as a rank-one orthogonal projection:

$$Q = |\psi\rangle\langle\psi| = \frac{1}{2} \begin{pmatrix} 1 + z & x + iy \\ x - iy & 1 - z \end{pmatrix}$$

with $x, y, z \in \mathbb{R}$, $x^2 + y^2 + z^2 = 1$. 

Bloch sphere
Matrix and Bloch sphere

- It is convenient to represent the quantum state $|\psi\rangle$ as a rank-one orthogonal projection:

$$Q = |\psi\rangle\langle\psi| = \frac{1}{2} \begin{pmatrix} 1 + z & x + iy \\ x - iy & 1 - z \end{pmatrix}$$

with $x, y, z \in \mathbb{R}$, $x^2 + y^2 + z^2 = 1$.

- The state of $k$ qubits are convex sum of $2^k \times 2^k$ matrices of the form $|\psi\rangle\langle\psi|$ with $|\psi\rangle = |x_1 \cdots x_k\rangle$. 

Bloch sphere
Mathematical tools

- As a consequence of the Schrödinger equation
Mathematical tools

- As a consequence of the Schrödinger equation

All quantum gates and quantum evolutions (for a closed system) are
Mathematical tools

• **As a consequence of the Schrödinger equation**
  All quantum gates and quantum evolutions (for a closed system) are unitary similarity transforms of the density matrices representing the states, i.e.,

  \[ A(t) \mapsto U(t)A(0)U(t)^* \]

  for some unitaries \( U(t) \).
Mathematical tools

- **As a consequence of the Schrödinger equation**
  All quantum gates and quantum evolutions (for a closed system) are unitary similarity transforms of the density matrices representing the states, i.e.,
  \[ A(t) \mapsto U(t)A(0)U(t)^* \]
  for some unitaries \( U(t) \).

- **By the results of Choi in 70’s and Kraus in 80’s**
  Quantum channels, quantum operations, quantum measurement operators, etc. are
Mathematical tools

- **As a consequence of the Schrödinger equation**
  All quantum gates and quantum evolutions (for a closed system) are unitary similarity transforms of the density matrices representing the states, i.e.,
  \[ A(t) \mapsto U(t)A(0)U(t)^* \]
  for some unitaries \( U(t) \).

- **By the results of Choi in 70’s and Kraus in 80’s**
  Quantum channels, quantum operations, quantum measurement operators, etc. are trace preserving completely positive linear maps of the form
  \[ A \mapsto \sum_{j=1}^r F_j AF_j^*. \]
Mathematical tools

- **As a consequence of the Schrödinger equation**
  All quantum gates and quantum evolutions (for a closed system) are unitary similarity transforms of the density matrices representing the states, i.e.,
  \[ A(t) \mapsto U(t)A(0)U(t)^* \]
  for some unitaries \( U(t) \).

- **By the results of Choi in 70’s and Kraus in 80’s**
  Quantum channels, quantum operations, quantum measurement operators, etc. are trace preserving completely positive linear maps of the form
  \[ A \mapsto \sum_{j=1}^{r} F_j AF_j^* \].

- **The theory was discovered way before the applications!**
Quantum complexity

- For $k = 100$, we have a state represented as a convex sum of matrices corresponding to $|\psi\rangle = |x_1 \cdots x_{100}\rangle$ of size

$$2^{100} = (2^{10})^{10} \approx 10^{30}.$$
Quantum complexity

- For \( k = 100 \), we have a state represented as a convex sum of matrices corresponding to \( |\psi\rangle = |x_1 \cdots x_{100}\rangle \) of size

\[
2^{100} = (2^{10})^{10} \approx 10^{30}.
\]

- If a high speed computer can do \( 10^{15} \) operations per second, to do one operation on each of the states corresponding to \( |\psi\rangle\langle\psi| \),

...
Quantum complexity

- For $k = 100$, we have a state represented as a convex sum of matrices corresponding to $|\psi\rangle = |x_1 \cdots x_{100}\rangle$ of size

$$2^{100} = (2^{10})^{10} \approx 10^{30}.$$  

- If a high speed computer can do $10^{15}$ operations per second, to do one operation on each of the states corresponding to $|\psi\rangle \langle \psi|$, one needs

$$10^{30} / 10^{15} = 10^{15} \text{ seconds},$$

which is more than 300,000 centuries!
Quantum complexity

- For $k = 100$, we have a state represented as a convex sum of matrices corresponding to $|\psi\rangle = |x_1 \cdots x_{100}\rangle$ of size $2^{100} = (2^{10})^{10} \approx 10^{30}$.

- If a high speed computer can do $10^{15}$ operations per second, to do one operation on each of the states corresponding to $|\psi\rangle\langle\psi|$, one needs $10^{30}/10^{15} = 10^{15}$ seconds, which is more than 300,000 centuries!

- That is why Feyman in 1980’s suggested that one could not simulate quantum systems using digital computer.
Quantum algorithms

- Step 1. Create a maximal entangled state:

\[ |\psi\rangle = 2^{-k/2} \sum |x_1 \cdots x_k\rangle, \quad x_j \in \{0, 1\}. \]
Quantum algorithms

- Step 1. Create a maximal entangled state:

\[ |\psi\rangle = 2^{-k/2} \sum |x_1 \cdots x_k\rangle, \quad x_j \in \{0, 1\}. \]

- Step 2. Apply an (unitary) operation \( f \) to \( |\psi\rangle \) to get

\[ f(|\psi\rangle) = 2^{-k/2} \sum f(|x_1 \cdots x_k\rangle). \]
Quantum algorithms

• Step 1. Create a maximal entangled state:

$$|\psi\rangle = 2^{-k/2} \sum |x_1 \cdots x_k\rangle, \quad x_j \in \{0, 1\}.$$  

• Step 2. Apply an (unitary) operation $f$ to $|\psi\rangle$ to get

$$f(|\psi\rangle) = 2^{-k/2} \sum f(|x_1 \cdots x_k\rangle).$$

• Step 3. Choose a suitable unitary operator $g$ so that

$$g(f(|\psi\rangle)) = |y\rangle \otimes |z\rangle,$$

where $|y\rangle$ will carry some useful information.
Deutsch-Jozsa algorithm

- In 1985, David Deutsch used the superposition idea to design an algorithm to determine whether a function $f : \{|0\rangle, |1\rangle\} \rightarrow \{|0\rangle, |1\rangle\}$ satisfies:

$$f(|0\rangle) = f(|1\rangle) \quad \text{or} \quad f(|0\rangle) \neq f(|1\rangle).$$
Deutsch-Jozsa algorithm

- In 1985, David Deutsch used the superposition idea to design an algorithm to determine whether a function $f : \{|0\rangle, |1\rangle\} \rightarrow \{|0\rangle, |1\rangle\}$ satisfies:

$$f(|0\rangle) = f(|1\rangle) \quad \text{or} \quad f(|0\rangle) \neq f(|1\rangle).$$

- In classical computing, one must compute $f(|0\rangle)$ and $f(|1\rangle)$ to answer the above question.
In 1992, David Deutsch and Richard Jozsa extended the algorithm to determine whether a function
\[ f : \{|x_1 \cdots x_n\} : x_i = 0 \text{ or } 1 \rightarrow \{|↑\}, |↓\} \]
is constant of balanced.
In 1992, David Deutsch and Richard Jozsa extended the algorithm to determine whether a function

\[ f : \{ |x_1 \cdots x_n \rangle : x_i = 0 \text{ or } 1 \} \rightarrow \{ |\uparrow\rangle, |\downarrow\rangle \} \]

is constant of balanced.

The Deutsch-Jozsa algorithm has been implemented:
• In 1992, David Deutsch and Richard Jozsa extended the algorithm to determine whether a function 
\[ f : \{|x_1 \cdots x_n\} : x_i = 0 \text{ or } 1 \rightarrow \{|↑\rangle, |↓\rangle\} \]
is constant of balanced.

• The Deutsch-Jozsa algorithm has been implemented:

Shor’s algorithm

- In 1994, Shor designed a quantum algorithm to factor an integer \( N = pq \) for two large prime numbers \( p \) and \( q \) in polynomial time of \( \log N \).
Shor’s algorithm

- In 1994, Shor designed a quantum algorithm to factor an integer \( N = pq \) for two large prime numbers \( p \) and \( q \) in polynomial time of \( \log N \).

- This is exponentially faster than the most efficient known classical factoring algorithm, the general number field sieve, which works in sub-exponential time — about \( O\left(e^{\left(\log N\right)^{1/3}\left(\log \log N\right)^{2/3}}\right) \).
Shor’s algorithm

- In 1994, Shor designed a quantum algorithm to factor an integer \( N = pq \) for two large prime numbers \( p \) and \( q \) in polynomial time of \( \log N \).

- This is exponentially faster than the most efficient known classical factoring algorithm, the general number field sieve, which works in sub-exponential time – about \( O \left( e^{(\log N)^{1/3} (\log \log N)^{2/3}} \right) \).

- Shor’s algorithm is important because it can be used to “break” the widely used public-key cryptology scheme known as RSA, which is based on the assumption that factoring large numbers is computationally infeasible (by classical computers).
Implementation

- In 2001, Shor’s algorithm was demonstrated by a group at IBM, who factored 15 into $3 \times 5$, using an NMR quantum computer with 7 qubits.
Implementation

- In 2001, Shor’s algorithm was demonstrated by a group at IBM, who factored 15 into $3 \times 5$, using an NMR quantum computer with 7 qubits.

- However, some doubts have been raised as to whether IBM’s experiment was a true demonstration of quantum computation, since no entanglement was observed.
Implementation

• In 2001, Shor’s algorithm was demonstrated by a group at IBM, who factored 15 into $3 \times 5$, using an NMR quantum computer with 7 qubits.

• However, some doubts have been raised as to whether IBM’s experiment was a true demonstration of quantum computation, since no entanglement was observed.

• Since IBM’s implementation, several other groups have implemented Shor’s algorithm using photonic qubits, emphasizing that entanglement was observed in 2007.
**Decoherence**

*Quantum decoherence* is a result of a quantum system interacting with its environment.

![Diagram showing decoherence process](image)
Decoherence

**Quantum decoherence** is a result of a quantum system interacting with its environment.

When qubits go through a quantum channel, they are subject to decoherence.
Quantum error correction

• One has to build suitable hardware and design efficient quantum error correcting schemes to overcome the decoherence problem.
Quantum error correction

- One has to build suitable hardware and design efficient quantum error correcting schemes to overcome the decoherence problem.

- Classical error correction employs redundancy, which is impossible for quantum computing by no-cloning theorem.

\[(1) \rightarrow (11111) \rightarrow (11101) \rightarrow (11111) \rightarrow (1).\]

[Encode] [Transmit] [Correct] [Decode]
Quantum error correction

- One has to build suitable hardware and design efficient quantum error correcting schemes to overcome the decoherence problem.
- Classical error correction employs redundancy, which is impossible for quantum computing by no-cloning theorem.

\[
1 \rightarrow (11111) \rightarrow (11101) \rightarrow (11111) \rightarrow 1.
\]

[Encode] [Transmit] [Correct] [Decode]

- One uses entanglement, algebraic coding theory, and operator theory techniques to deal with the problem.
Quantum error correction

- One has to build suitable hardware and design efficient **quantum error correcting schemes** to overcome the **decoherence** problem.

- Classical error correction employs redundancy, which is impossible for quantum computing by **no-cloning theorem**.

\[
(1) \rightarrow (11111) \rightarrow (11101) \rightarrow (11111) \rightarrow (1).
\]

[Encode] [Transmit] [Correct] [Decode]

- One uses **entanglement**, **algebraic coding theory**, and **operator theory techniques** to deal with the problem.

- Knill, Laflamme, Steane, Shor, Calderbank, Sloane, Choi, Kribs, Holbrook, Li, Poon, Sze, ....
Quantum cryptology

- Alice and Bob want to communicate in a secure way so that Eve (the notorious eavesdropper) cannot listen or modify the message.
Quantum cryptology

- Alice and Bob want to communicate in a secure way so that Eve (the notorious eavesdropper) cannot listen or modify the message.

- **Quantum cryptology** provides a scheme for Alice and Bob to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.
Quantum cryptology

- Alice and Bob want to communicate in a secure way so that Eve (the notorious eavesdropper) cannot listen or modify the message.

- **Quantum cryptology** provides a scheme for Alice and Bob to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

- For example, the key is \( k = (10110011100011110000) \). Every message \( m = (x_1 x_2 \cdots x_{20}) \) is encrypted and decrypted as follows: [encrypt] \( \rightarrow \) [transmit/correct] \( \rightarrow \) [decrypt]

\[
m \rightarrow m \oplus k \rightarrow m \oplus k \rightarrow (m \oplus k) \oplus k = m.
\]
Quantum cryptology

- Alice and Bob want to communicate in a secure way so that Eve (the notorious eavesdropper) cannot listen or modify the message.

- **Quantum cryptology** provides a scheme for Alice and Bob to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

  - For example, the key is $k = (1011001110011110000)$. Every message $m = (x_1 x_2 \cdots x_{20})$ is encrypted and decrypted as follows:
    
    $[\text{encrypt}] \rightarrow [\text{transmit/correct}] \rightarrow [\text{decrypt}]
    \begin{align*}
    m & \rightarrow m \oplus k \\
    m \oplus k & \rightarrow (m \oplus k) \oplus k = m.
    \end{align*}

- There will be no eavesdropping (observing will change the quantum states) and no way to fake information (no cloning).
BB84 Protocol

BB84 Protocol


- Alice sends Bob $4N$ photons.
BB84 Protocol


- Alice sends Bob $4N$ photons.
- Alice (Bob) randomly chooses one of the two bases to send (measure) each photon.
BB84 Protocol


- Alice sends Bob $4N$ photons.
- Alice (Bob) randomly chooses one of the two bases to send (measure) each photon.
- Exchange the information in the $4N$ qubits by by classical channel (unsecured) to identify roughly $2N$ of the photons were sent and received by the same bases.
BB84 Protocol


- Alice sends Bob $4N$ photons.
- Alice (Bob) randomly chooses one of the two bases to send (measure) each photon.
- Exchange the information in the $4N$ qubits by by classical channel (unsecured) to identify roughly $2N$ of the photons were sent and received by the same bases.
- Check the errors in $N$ of the remaining $2N$ photons by classical channel (unsecured) to ensure no eavesdropper, and the bit strings in the other $N$ photons can be used. Else, repeat the process.
Implementation

- There are different research groups developing the technology.
Implementation

- There are different research groups developing the technology.
- There are currently at least four companies offering commercial quantum cryptography systems.
Implementation

- There are different research groups developing the technology.
- There are currently at least four companies offering commercial quantum cryptography systems.
- In Vienna, Austria, bank transfer using quantum cryptology was first done in 2004, and a security computer network was set up in 2008.
Quantum teleportation

It is a technique using quantum entanglement to transfer information on a quantum level.
Quantum teleportation

It is a technique using quantum entanglement to transfer information on a quantum level. (See the Youtube clip.)
Quantum teleportation

It is a technique using quantum entanglement to transfer information on a quantum level. (See the Youtube clip.)

Controversies about entanglement
Quantum teleportation

It is a technique using quantum entanglement to transfer information on a quantum level. (See the Youtube clip.)

Controversies about entanglement

- Einstein, Podolsky, and Rosen, who introduced the thought experiment in a 1935 paper to argue that quantum mechanics is not a complete physical theory.
Quantum teleportation

It is a technique using quantum entanglement to transfer information on a quantum level. (See the Youtube clip.)

Controversies about entanglement

- Einstein, Podolsky, and Rosen, who introduced the thought experiment in a 1935 paper to argue that quantum mechanics is not a complete physical theory.
- Most physicists today regard the EPR paradox as an illustration of how quantum mechanics violates classical intuitions.
Quantum teleportation

It is a technique using quantum entanglement to transfer information on a quantum level. (See the Youtube clip.)

Controversies about entanglement

• Einstein, Podolsky, and Rosen, who introduced the thought experiment in a 1935 paper to argue that quantum mechanics is not a complete physical theory.

• Most physicists today regard the EPR paradox as an illustration of how quantum mechanics violates classical intuitions.

• Einstein never accepted quantum mechanics as a “real” and complete theory, struggling to the end of his life.
Quantum teleportation

It is a technique using quantum entanglement to transfer information on a quantum level. (See the Youtube clip.)

Controversies about entanglement

- Einstein, Podolsky, and Rosen, who introduced the thought experiment in a 1935 paper to argue that quantum mechanics is not a complete physical theory.
- Most physicists today regard the EPR paradox as an illustration of how quantum mechanics violates classical intuitions.
- Einstein never accepted quantum mechanics as a “real” and complete theory, struggling to the end of his life.
- As he once said: “God does not play dice.”
Conclusion

- Quantum Information Science concerns the study of QC, QC, QC.
Conclusion

- Quantum Information Science concerns the study of QC, QC, QC.
- It was a dream in 1980’s, and there has been much controversies.
Conclusion

- Quantum Information Science concerns the study of QC, QC, QC.
- It was a dream in 1980’s, and there has been much controversies.
- Because of the efforts of many researchers from different areas, much progress has been made.
Conclusion

- Quantum Information Science concerns the study of QC, QC, QC.
- It was a dream in 1980’s, and there has been much controversies.
- Because of the efforts of many researchers from different areas, much progress has been made.
- Quantum cryptology will be used widely in the near future.
Conclusion

• Quantum Information Science concerns the study of QC, QC, QC.
• It was a dream in 1980’s, and there has been much controversies.
• Because of the efforts of many researchers from different areas, much progress has been made.
• Quantum cryptology will be used widely in the near future.
• Quantum computing is in its infancy, but has a promising prospect.

Thank you
Conclusion

- Quantum Information Science concerns the study of QC, QC, QC.
- It was a dream in 1980’s, and there has been much controversies.
- Because of the efforts of many researchers from different areas, much progress has been made.
- Quantum cryptology will be used widely in the near future.
- Quantum computing is in its infancy, but has a promising prospect.
- Much theoretical work has been done on quantum complexity theory.

Thank you
Conclusion

• Quantum Information Science concerns the study of QC, QC, QC.
• It was a dream in 1980’s, and there has been much controversies.
• Because of the efforts of many researchers from different areas, much progress has been made.
• Quantum cryptology will be used widely in the near future.
• Quantum computing is in its infancy, but has a promising prospect.
• Much theoretical work has been done on quantum complexity theory.
• Stay tuned for the transformation, or join the workforce to explore these new frontiers!
Thank you for your attention!